PRIVACY IMPACT ASSESSMENT (PIA)

For the

Continuous Evaluation Records
Defense Manpower Data Center (DMDC)

SECTION 1: IS A PIA REQUIRED?

a. Will this Department of Defense (DoD) information system or electronic collection of information (referred to as an "electronic collection" for the purpose of this form) collect, maintain, use, and/or disseminate PII about members of the public, Federal personnel, contractors or foreign nationals employed at U.S. military facilities internationally? Choose one option from the choices below. (Choose (3) for foreign nationals).

☐ (1) Yes, from members of the general public.

☒ (2) Yes, from Federal personnel* and/or Federal contractors.

☐ (3) Yes, from both members of the general public and Federal personnel and/or Federal contractors.

☐ (4) No

* "Federal personnel" are referred to in the DoD IT Portfolio Repository (DITPR) as "Federal employees."

b. If "No," ensure that DITPR or the authoritative database that updates DITPR is annotated for the reason(s) why a PIA is not required. If the DoD information system or electronic collection is not in DITPR, ensure that the reason(s) are recorded in appropriate documentation.

c. If "Yes," then a PIA is required. Proceed to Section 2.

SECTION 2: PIA SUMMARY INFORMATION

a. Why is this PIA being created or updated? Choose one:

☒	**New DoD Information System**	☐	**New Electronic Collection**
☐	**Existing DoD Information System**	☐	**Existing Electronic Collection**
☐	**Significantly Modified DoD Information System**		

b. Is this DoD information system registered in the DITPR or the DoD Secret Internet Protocol Router Network (SIPRNET) IT Registry?

☐	**Yes, DITPR**	Enter DITPR System Identification Number	
☐	**Yes, SIPRNET**	Enter SIPRNET Identification Number	
☒	**No**		

c. Does this DoD information system have an IT investment Unique Project Identifier (UPI), required by section 53 of Office of Management and Budget (OMB) Circular A-11?

☐ **Yes** ☒ **No**

If "Yes," enter UPI

If unsure, consult the Component IT Budget Point of Contact to obtain the UPI.

d. Does this DoD information system or electronic collection require a Privacy Act System of Records Notice (SORN)?

A Privacy Act SORN is required if the information system or electronic collection contains information about U.S. citizens or lawful permanent U.S. residents that is retrieved by name or other unique identifier. PIA and Privacy Act SORN information should be consistent.

☒ **Yes** ☐ **No**

If "Yes," enter Privacy Act SORN Identifier DMDC 17 DoD

DoD Component-assigned designator, not the Federal Register number.
Consult the Component Privacy Office for additional information or
access DoD Privacy Act SORNs at: http://www.defenselink.mil/privacy/notices/

or

Date of submission for approval to Defense Privacy Office
Consult the Component Privacy Office for this date.

e. Does this DoD information system or electronic collection have an OMB Control Number?
Contact the Component Information Management Control Officer or DoD Clearance Officer for this information.

This number indicates OMB approval to collect data from 10 or more members of the public in a 12-month period regardless of form or format.

☐ **Yes**

Enter OMB Control Number

Enter Expiration Date

☒ **No**

f. Authority to collect information. A Federal law, Executive Order of the President (EO), or DoD requirement must authorize the collection and maintenance of a system of records.

(1) If this system has a Privacy Act SORN, the authorities in this PIA and the existing Privacy Act SORN should be the same.

(2) Cite the authority for this DoD information system or electronic collection to collect, use, maintain and/or disseminate PII. (If multiple authorities are cited, provide all that apply.)

(a) Whenever possible, cite the specific provisions of the statute and/or EO that authorizes the operation of the system and the collection of PII.

(b) If a specific statute or EO does not exist, determine if an indirect statutory authority can be cited. An indirect authority may be cited if the authority requires the operation or administration of a program, the execution of which will require the collection and maintenance of a system of records.

(c) DoD Components can use their general statutory grants of authority ("internal housekeeping") as the primary authority. The requirement, directive, or instruction implementing the statute within the DoD Component should be identified.

5 U.S.C. 9101, Access to Criminal History Information for National Security and Other Purposes; 10 U.S. C. 137, Under Secretary of Defense for Intelligence; 10 U.S.C. 504, Persons Not Qualified; 10 U.S.C. 505, Regular components: qualifications, term, grade; E.O. 10450, Security Requirements for Government Employment; E.O. 10865, Safeguarding Classified Information Within Industry; E.O. 12333, United States Intelligence Activities; E.O. 13526, Classified National Security Information; E.O. 12968, as amended, Access to Classified Information; E.O.13467, Reforming Processes Related to Suitability for Government Employment, Fitness for Contractor Employees, and Eligibility for Access to Classified National Security Information; E.O. 13470, Further Amendments to Executive Order 12333; 32 CFR part 154, Department of Defense Personnel Security Program Regulation; 32 CFR part 155, Defense Industrial Personnel Security Clearance; 32 CFR part 156, Department of Defense Personnel Security Program (DoDPSP); DoD Directive 1145.03E, United States Military Entrance Processing Command (USMEPCOM); DoD Instruction (DoDI) 1304.26, Qualification Standards for Enlistment, Appointment and Induction; DoDI 5200.02, DoD Personnel Security Program (PSP); DoDI 5220.06, Defense Industrial Personnel Clearance Review Program; DODI 5220.22, National Industrial Security Program (NISP); DoD 5200.2-R, Department of Defense Personnel Security Program Regulation; HSPD 12: Policy for a Common Identification Standard for Federal Employees and Contractors; FIPS 201-1: Personal Identity Verification (PIV) of Federal Employees and Contractors; Director of Central Intelligence Directive 8/1: Intelligence Community Policy on Intelligence Information Sharing; and E.O. 9397 (SSN), as amended.

g. Summary of DoD information system or electronic collection. Answers to these questions should be consistent with security guidelines for release of information to the public.

(1) Describe the purpose of this DoD information system or electronic collection and briefly describe the types of personal information about individuals collected in the system.

Records in the system will be used to conduct CE to: (1) identify DoD-affiliated personnel with eligibility for access to classified information who have engaged in conduct of security concern; (2) identify and initiate needed follow-on inquiries and/or investigative activity and enable security officials and adjudicators to determine and take appropriate actions; and (3) perform research, development, and analyses related to DoD's CE program. These analyses are conducted to: (a) evaluate and improve DoD and federal personnel security, insider threat, and other background vetting and continuous evaluation procedures, programs, and policies; (b) assist in providing training, instruction, and advice on personnel security and insider threats, and assess continuing reliability of subjects; (c) encourage cooperative research within and among DoD Components, the Intelligence Community, and the Executive branch on initiatives having DoD or Federal Government-wide implications in order to ensure that appropriate information is shared efficiently when authorized to do so and to avoid duplication of efforts; (d) address items of special interest to personnel security officials within DoD Components, the Intelligence Community, and the Executive branch (e.g., evaluating responses to excessive indebtedness, auditing information to ensure individuals with mental health issues are being protected appropriately, monitoring numbers and types of security incidents); and (e) conduct personnel security pilot test projects related to DoD's CE program for purposes of research and development.

The types of information about individuals collected in this system include: Responses from official questionnaires (e.g. SF 86 Questionnaire for National Security Positions) that include Names, Social Security Number, Other ID Numbers, Date and location of birth, demographic information, spouse information, education information, financial information, employment information citizenship information and contact information; records of personnel background investigations; information contained in local, state or Federal criminal justice records.

(2) Briefly describe the privacy risks associated with the PII collected and how these risks are addressed to safeguard privacy.

Privacy risk associated with the PII collection includes unauthorized access to information, which could result in risks such as identity theft, harassment or blackmail. This risk is reduced by incorporating role-based access procedures to personal information, which includes limiting access only to those who require it in the performance of their official duties. All individual's accessing personal information must have a need-to-know, have a security clearance eligibility level equal to or higher than subjects of records to which they have access, have been advised of the sensitivity of the records and their responsibilities to safeguard the information from unauthorized disclosure.

Additionally, all data transfers and information retrievals using remote communication facilities are encrypted. Records are maintained in a secure database in a controlled environment accessible only to authorized personnel.

h. With whom will the PII be shared through data exchange, both within your DoD Component and outside your Component (e.g., other DoD Components, Federal Agencies)? Indicate all that apply.

☒ **Within the DoD Component.**

Specify. Joint Personnel Accounting System, Defense Logistics Agency, Central Adjudication Tracking System

☒ **Other DoD Components.**

Specify. United States Army G-2

☒ **Other Federal Agencies.**

Specify. Federal Bureau of Investigations, National Crime Information Center; Office of Personnel Management; Office of the Director of National Intelligence

☒ **State and Local Agencies.**

Specify. Data may be provided to state and local agencies, if necessary, to obtain information from them, which will assist in identifying security risks in the personnel security field. Data may also be exchanged as per required with state and local agencies, if failure to exchange would constitute a violation of federal law.

☐ **Contractor** (Enter name and describe the language in the contract that safeguards PII.)

Specify.

☒ **Other** (e.g., commercial providers, colleges).

Specify. iMapData, Equifax, Thomas Reuters Special Services (TRSS)

i. Do individuals have the opportunity to object to the collection of their PII?

☒ **Yes** ☐ **No**

(1) If "Yes," describe method by which individuals can object to the collection of PII.

Information provided by individuals for a security clearance is voluntary. However, the Department may not be able to complete an investigation, or complete it in a timely manner, if the individual does not provide the necessary information. The individual authorizes the collection and use of their data for Continuous Evaluation purposes by completing and signing the SF86 (2010 Edition).

(2) If "No," state the reason why individuals cannot object.

j. Do individuals have the opportunity to consent to the specific uses of their PII?

☒ **Yes** ☐ **No**

(1) If "Yes," describe the method by which individuals can give or withhold their consent.

By signing the SF 86 (2010 Edition), the individuals consents to Continuous Evaluation.

(2) If "No," state the reason why individuals cannot give or withhold their consent.

k. What information is provided to an individual when asked to provide PII data? Indicate all that apply.

☐	**Privacy Act Statement**	☐	**Privacy Advisory**
☐	**Other**	☒	**None**

Describe each applicable format.

Continuous Evaluation does not collect information directly from the individual.